Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

REMARKS/ARGUMENTS

Claims 1-24 are pending in this application. Claims 1-24 were rejected under 35 U.S.C. §103(a) as being unpatentable over Candelore (6,383,149) in view of Hoffman et al. (5,613,012).

Specification Amendments

The specification has been amended to clarify the related applications that are incorporated by reference. There was an inadvertent duplication of an application as well as a reference to the present application in the incorporation by reference claim. Those portions have been deleted and the application numbers requested by the Examiner have been added.

Section 103 Issues

The Office Action rejected claims 1-24 by combining the Candelore reference with the Hoffman reference. In regard to claim 1, the Office Action referenced the abstract, figs. 1-3, col. 10, lines 33-67; col. 11 and col. 12, lines 1-14 of the Candelore reference. Notably, these sections of Candelore describe the <u>subscriber</u> side of the system rather than the encryption renewal system side of the system. Fig. 1 describes an entertainment system for receiving program data from a service provider, such as a cable operator. Thus, it is clearly the subscriber side. Fig. 2 is stated to be a block diagram of the digital receiver 111. See Col. 5 at lines 46-47. Therefore, it is clearly describing the subscriber side. Fig. 3 describes a block diagram of the conditional access unit 240 shown in Fig. 2. Thus, it is describing the conditional access unit that is part of the digital receiver. Therefore, it is part of the subscriber side of the system. Consequently, Figs. 1-3 and their accompanying description do not teach the embodiment claimed in claim 1.

Similarly, col. 10, lines 33-67, column 11, and column 12, lines 1-14 recites:

"FIGS. 6B through 6E show embodiments for recording future access keys. FIG. 6A shows a conventional entitlement control message. The key used to descramble the content is encrypted

Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

under the current group or service key, which is sent in the ECM 610. The scrambled content may be recorded. However, the key may expire after a period of time. If a customer tries to view the recorded scrambled content at a later time, the conditional access element may not be able to recover the content if the key has expired. This is how payment is enforced by the service provider.

FIG. 6B shows one embodiment of entitlement control messages (ECMs) that contain fields encrypting future delivered group or service keys. In this embodiment, multiple ECMs are created and recorded along with the content. Each ECM 660 contains a key that corresponds to a given time period. In FIG. 6B, time X is the current key epoch, while time X-1 is the next epoch. If a customer were authorized to view an entire year of content, and if keys changed on a monthly epoch basis, then 12 different ECMs could be generated, included in the data stream, and recorded along with the content. Thus, a customer could record the content, and still have access to view the content for one year.

FIG. 7A shows a flow diagram for one embodiment of creating the ECMs of FIG. 6B. One or more keys are created, 710. A time period is assigned to each key, where the time period may be a past, present, or future time period, 720. A plurality of entitlement control messages are created so that each entitlement control message corresponds to a given time period, 730. For each key, place the key assigned to a given time period in the ECM corresponding to the given time period, 740. The content of a program, together with the plurality of ECMs, are recorded, 750. During a given time period, the key from the ECM that

Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

corresponds to the given time period is used to descramble the content of a program, 760.

FIGS. 6C and 6D show another embodiment of an entitlement control message. Here, one ECM 674 is created, and includes multiple keys corresponding to multiple time periods. In FIG. 6C, each encrypted key may correspond to a monthly time period, for example. In FIG. 6D, ECM 675 has key information encrypted under several keys. Key 684 is the current group or service key. Keys 685, 686 are time keys. They are not based on the same time epoch as the group or service key, but instead are used for retrieval of stored content after the most recent epoch or epochs have expired. A time key may be a vintage key. A vintage key may unlock all material from a particular group or service after a certain amount of time has elapsed, for example, two or three years. This reduces the number of fields of encrypted key information, therefore, ECMs could be made shorter to conserve bandwidth.

FIG. 6E shows another embodiment of the format of an entitlement control message 675. This relies on a simple coverage key 687 that either never changes unless there is a security problem or break, or changes extremely slowly, for example, on the order of years. The ECM access requirements 631 contain all the necessary information in order to recover the program. This format may rely on the ECM signature 650 to verify that none of the access conditions have been modified. This embodiment may benefit from public key cryptography, where the key used to decrypt or verify is not the key used to encrypt or sign messages. A conditional access element that has been compromised and

Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

thoroughly analyzed would not necessarily break the system for all

conditional elements. The public key system would need to be

broken as well. In the case of public key cryptography, the simple

coverage key might not be required, as the key field along with

other data could be encrypted with the signature.

FIG. 7B shows a flow diagram of a method for creating one

entitlement control message with a plurality of keys. In step 765, a

plurality of keys are created. One or more time periods are

assigned to each key, where each time period may be a past,

present or future time period, 770. Create one entitlement control

message, step 775. The plurality of keys are placed in the

entitlement control message, 780. The content of a program is

recorded together with the entitlement control message, 785.

During a given time period, the content of a program is scrambled.

The scrambled content is transmitted, or delivered to a user, 790,

along with the ECM, by delivering the content to a conditional

access unit. Transmit the scrambled content and the entitlement

control message to a conditional access unit, step 795. The content

is descrambled using the appropriate key for the given time period

from the ECM, 797.

The present invention may also track entitlements over time. For

example, a new customer may be currently subscribed to a service,

and is therefore entitled to view content delivered during the

current billing period. However, the customer may not be

authorized by the service to view content from previous periods.

Therefore, if the service provider does not want a customer to have

access to previously recorded content unless the customer pays for

Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

it, then the entitlement history of the customer has to be tracked.
Information on whether a subscriber was authorized to view a
service or package can be delivered in entitlement management
messages, along with other entitlement information, as shown in
FIG. 8A. ECM 810 includes information about entitlements that
the customer currently has, in field 830, as well as the customer's
entitlement time history 840.

FIG. 8B shows one embodiment of an entitlement management
message 850 that tracks a user's entitlement history in field 870.
This entitlement time history may be delivered along with key and
entitlement information. Each bit shown in the entitlement time
history field 870 represents whether or not a customer was
subscribed or authorized for a service for one or more discrete time
periods. Thus, the first bit shown in FIG. 8B may represent
whether a customer has access to content recorded 24 months ago.
If this bit is in a first state, which may be zero, for example, then
the customer may not view content from this time period, even if
the customer has the key information for this time period. The
memory required to store the entitlement time history information
can be reduced using this method. For example, two years worth of
information, with each bit representing one month, would only
require 24 bits or 3 bytes of storage along with the header 860."

Nothing in this quoted section teaches a first platform or a second platform as
recited in claim 1 of Applicant's application. Clearly, nothing in this quoted section teaches
"receiving a request to generate the entitlement control messages."

Thus, it is believed that the cited passages of Candelore do not stand for what the
Office Action asserted they stand for. Consequently, the rejection of claim 1 is respectfully

Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

traversed. Claim 2 depends from claim 1 and is believed to be allowable for the same reason(s) that claim 1 is allowable.

Claim 3 was rejected under the same analysis applied to claim 1. As was noted in the case of claim 1, the Candelore reference does not actually teach a first platform and a second platform as recited by claim 3. For at least this reason, the rejection of claim 3 is respectfully traversed. Claims 4-12 depend from claim 3 and are believed to be allowable for the same reason(s) that claim 3 is allowable.

Claim 13 was rejected under the same analysis applied to claim 1. Claim 13 is directed at an encryption renewal system. As evidenced by Fig. 1 of Applicant's specification, such an encryption renewal system does not occur on the subscriber side of the communication system. Therefore, the citation of Figs. 1-3 of Candelore is inapplicable. Furthermore, the other cited sections of Candelore at col. 10, lines 33-67, column 11, and column 12, lines 1-14 discuss ECM messages rather than EMM messages. EMM messages are recited in claim 13. Therefore, the rejection of claim 13 is respectfully traversed and claim 13 is believed to be in condition for allowance. Claims 14-16 depend from claim 13 and are believed to be allowable for the same reason(s) that claim 13 is allowable.

Claim 17 was rejected under the same analysis applied to claim 1. It is unclear as to where the Office Action actually addresses the elements of claim 17. For example, the Office Action does not address where either the Candelore reference or the Hoffman reference teaches "generating registration data for registering the off-line encryption device." For at least this reason, the rejection of claim 17 is respectfully traversed and claim 17 is believed to be in condition for allowance. Claims 18-24 depend from claim 17 and are therefore believed to be allowable for the same reason(s) as claim 17.

Combination of References

It is also noted that the Office Action in combining the Candelore and Hoffman references asserted that one could insert the firewalls of Hoffman into the Candelore reference. The Applicant respectfully notes that this would require a complete reconstruction of Candelore which is impermissible under 35 USC §103. The MPEP notes that an obviousness rejection

Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

cannot be made when the proposed combination of references would change the principle of operation of the cited reference. See, MPEP, Seventh Edition, Revision 1, February 2000, section 2143.02 at page 2100-99, citing In re Ratti, 123 USPQ 349 (CCPA 1959). In re Ratti also stands for the rule that the combination of references must not require substantial reconstruction or redesign of the references to arrive at the claimed invention. In the In re Ratti case, the Court of Customs and Patent Appeals reversed the rejection of the claims and emphasized that the modification of the prior art would be too substantial to have been obvious:

> "We hold . . . that the combination of Jepson with Chinnery et al. is not a proper ground for rejection of the claims here on appeal. This suggested combination of references would require a substantial reconstruction and redesign of the elements shown in Chinnery et al. as well as a change in the basic principles under which the Chinnery et al construction was designed to operate." In re Ratti, 123 USPQ 349, 352 (C.C.P.A 1959).

> "Once [applicant Ratti] had taught how this could be done, the redesign may, by hindsight, seem to be obvious to one having ordinary skills in the shaft sealing art. However, when viewed as of the time [applicant's] invention was made, and without the benefit of [applicant's] disclosure, we find nothing in the art of record which suggests appellants novel oil seal . . . ." Id. at 352.

In the present application, the combination of Candelore and Hoffman would require the physical separation of computing platforms and the insertion of a firewall. Such a drastic change is clearly the type of substantial reconstruction that the MPEP says is not permissible. (Again, it should be noted that Applicant traverses the suggestion that the cited portions of Candelore actually teach a first computing platform and a second computing platform as recited in Applicant's claim 1).

Thus, it is believed that the combination of the Candelore and Hoffman references is inapplicable and is therefore respectfully traversed.

Appl. No. 09/898,168
Amdt. dated May 12, 2005
Reply to Office Action of January 12, 2005

PATENT

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at 303-571-4000.

Respectfully submitted,

William F. Vobach
Reg. No. 39,411

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: 303-571-4000
Fax: 415-576-0300
WFV:klb
60412898 v1